Veiledning i kryptering med Open PGP

GNU Privacy Guard for Windows (Gpg4win) er en gratis programvare for kryptering av tekst, filer og eposter ved hjelp av standarden OpenPGP for Windows-operativsystem. OpenPGP er den mest brukte standarden for å kommunisere sensitive data over usikre elektroniske kommunikasjonsmidler.

Denne veiledningen[1] bruker Gpg4win og GNU Privacy Assistant som en løsning som ikke er bundet til en spesifikt e-postklient. Andre løsninger man kan vurdere er Enigmail for OpenPGP i Thunderbird, og Symantecs OpenPGP-produkter.

Hva er OpenPGP?

OpenPGP (RFC 4880[2]) er en standard for kryptering av digitale data, for eksempel e-poster og vedlegg. OpenPGP kan også benyttes til å digitalt signere tekst eller filer, og dermed bekrefte at dataene kommer fra den avsenderen du forventer.

Krypteringen foregår ved hjelp av en privat nøkkel (også kalt sertifikat) og en offentlig nøkkel. Den offentlige nøkkelen kan fritt deles ut, og for eksempel lastes opp og linkes til på nettsider. Den brukes av personer som ønsker å kommunisere kryptert med eller bekrefte at en melding kommer fra eieren av nøkkelen.

Den private nøkkelen brukes til å dekryptere meldinger sendt til brukeren, samt til å digitalt signere tekster og filer. Denne nøkkelen må ikke deles, og bør beskyttes med et sterkt passord. Alle som har tilgang til nøkkelen og dette passordet vil kunne dekryptere meldinger sendt kryptert til den offentlige nøkkelen, samt kunne utgi seg for å være den nøkkelen tilhører.

OpenPGP brukes av Datatilsynet til å kommunisere over usikre kanaler. Dette muliggjør utveksling av sensitiv og fortrolig informasjon over e-post, og sikrer at sender og mottaker kan være trygge på at innholdet i e-posten ikke har blitt lest eller redigert av en tredjepart.

Informasjon som kan være vesentlig å kryptere er blant annet:

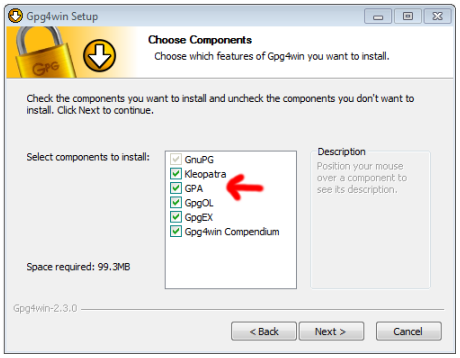
- forhåndsdrøftelser
- avvik som er delt under TLP-protokollen[3] nivå **[TLP:GUL / TLP:AMBER]** eller høyere
- sensitiv informasjon etter personopplysningsloven, og
- fortrolig virksomhetsinformasjon

OpenPGP er **ikke** godkjent for overføring av gradert informasjon underlagt sikkerhetsloven.

[1] Veiledningen er basert på NSM's veiledning om Innføring i bruk av Gpgp4win, versjon 1.3
[2] https://tools.ietf.org/html/rfc4880
[3] https://nsm.stat.no/norcert/kontakt-operasjonssenteret/trafikklysprotokollen---tlp/

Hvordan installere Gpg4win

Gpg4win kan lastes ned fra https://www.gpg4win.org/download.html. Under installasjonen av Gpg4win får man flere installasjonsmuligheter – i denne veiledningen benyttes GPA, huk derfor av for GPA.



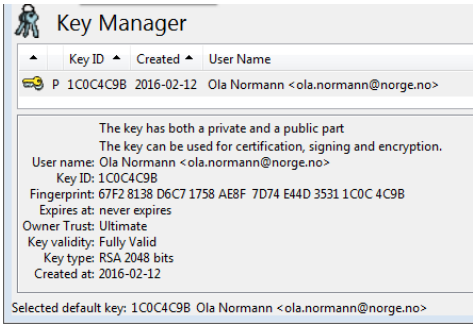
Figur 1: Skjermbilde fra Gpg4win installasjon

Når installasjonen er ferdig starter man GPA fra Start-menyen. Dersom Key Manager ikke åpner seg ved første gangs bruk, åpne den fra menylinjen: Windows => Key Manager.

Nøkkelbehandling

Verifisering av OpenPGP-nøkler

OpenPGP-nøkler verifiseres vanligvis over telefon eller personlig oppmøte ved å sammenligne et fingeravtrykk/fingerprint. Det viktigste er at fingeravtrykk verifiseres over en annen kommunikasjonskanal enn der man mottok nøkkelen. Dette er for å bekrefte at nøkkel ikke er blitt byttet ut. Fingeravtrykket oppgis som en heksadesimal tekststreng som vanligvis består av 40 tegn. Etter at man har generert eller importert en nøkkel kan man se detaljer, slik som fingerprint, ved å velge nøkkelen i Key Manager-visningen.



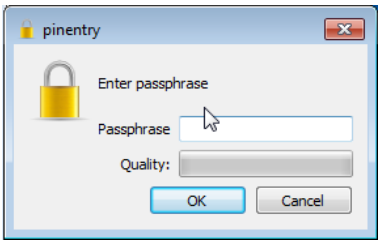
Figur 2: Skjermbilde nøkkel med detaljer vist

Lag et nytt sett med OpenPGP-nøkler

1. Key Manager-visningen av GPA åpnes som nevnt normalt automatisk første gang du åpner GPA. Du vil her få valget om å importere eller lage en ny nøkkel (eventuelt åpne GPA fra menylinjen: Windows => Key Manager => Keys => New key).
2. Tast inn informasjonen som skal identifisere nøkkelen. Dette vil vanligvis være ditt navn og din e-postadresse, eller et fellesnavn og en felles e-postadresse.
3. Velg at du ønsker å lage en kopi (backup) av nøkkelen til fil. Vi anbefaler at man lagrer en kopi av nøkkelen på en ekstern enhet, for eksempel en minnepinne eller annet medium

med lengre levetid, og deretter legger denne på et sikkert sted. Smartkort og papirkopier er også vanlige verktøy for langtidslagring.

4. Tast inn et passord for å beskytte nøkkelen. Du vil bli bedt om å repetere dette passordet én gang.

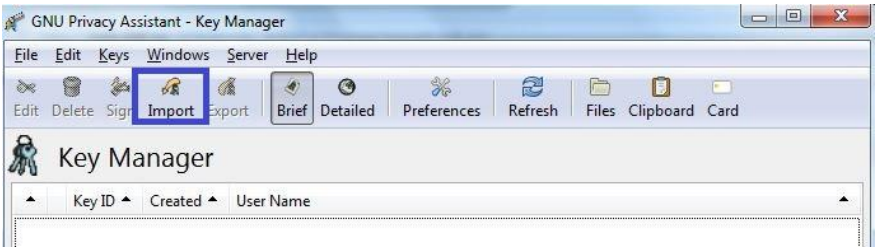


Figur 3: Skjermbilde av passorddialogen

Enhver som får tak i en kopi av nøkkelen og dette passordet, vil kunne dekryptere meldinger og signere data på vegne av denne nøkkelen.

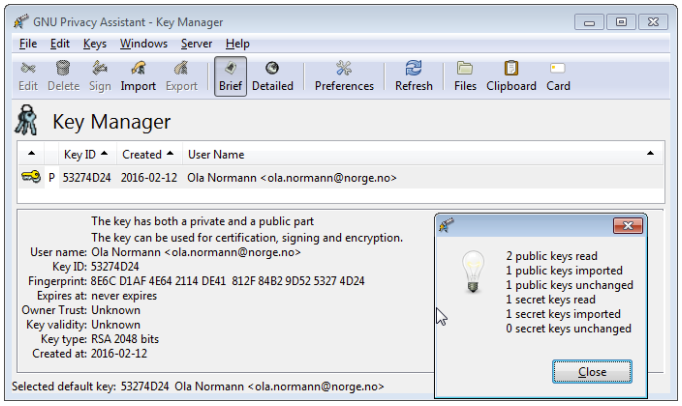
Importer din private nøkkel

1. Key Manager-visningen av GPA bør åpne første gang du åpner GPA. Du vil her få valget om å importere eller lage en ny nøkkel (eventuelt åpne GPA fra menylinjen: Windows => Key Manager).
2. Klikk Import-ikonet i hovedvinduet.



Figur 4: Skjermbilde fra Gpg4win import av nøkler

3. Naviger frem til din private nøkkel, og merk filen.
4. Klikk Open
5. GPA bør rapportere at minst én offentlig og én privat nøkkel ble importert.



Figur 5: GPA rapporterer at en offentlig og en privat nøkkel ble importert

6. Fordi dette er din nøkkel, men den er importert fra en ekstern kilde, vil ikke GPG stole på denne nøkkelen. Høyreklikk på nøkkelen, velg Set Owner Trust og deretter Ultimate for å bekrefte at du stoler 100% på nøkkelen.

Importer Datatilsynets offentlige nøkkel

Datatilsynets offentlige OpenPGP-nøkkel kan lastes ned fra våre hjemmesider, her ligger også vår fingerprint[4].

Denne nøkkelen kan brukes til å sende krypterte meldinger til Datatilsynet, samt å bekrefte at Datatilsynet er avsender av en mottatt melding.

1. Last ned nøkkelen fra lenken over.
2. Klikk **Import**-ikonet i hovedvinduet.
3. Naviger frem til lokasjonen der du lagret Datatilsynet-nøkkelen, og merk filen.

Figur 6: Importering av Datatilsynets offentlige nøkkel

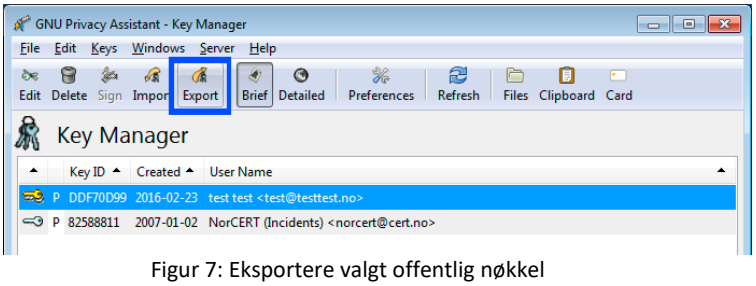
4. Klikk Open
5. GPA bør rapportere at en offentlig nøkkel ble importert.
6. Etter at du har bekreftet fingeravtrykket på Datatilsynets nøkkel kan du sette Owner Trust til et valgfritt nivå. Fingeravtrykket kan sjekkes ved å sammenligne med det oppgitt på våre hjemmesider, eller ved å kontakte oss via telefon.

De samme trinnene kan brukes for å importere OpenPGP-nøkler fra andre samarbeidspartnere

Eksporter din offentlige nøkkel

For at andre skal kunne kommunisere med deg via krypterte meldinger og vedlegg må de ha mottatt din offentlige nøkkel. Du kan enten sende nøkkelen til individuelle personer, eller du kan legge den offentlige nøkkelen på for eksempel en webside.

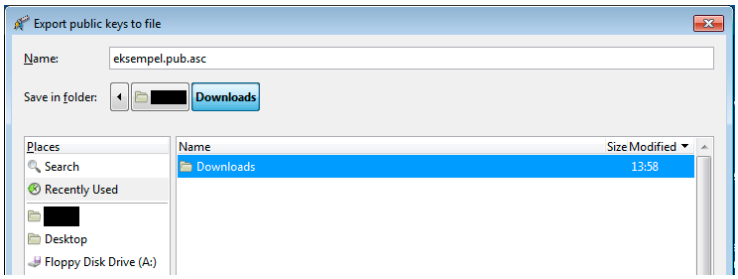
1. Velg ditt nøkkelpar i hovedvinduet som du vil eksportere.
2. Klikk Export-ikonet.



Figur 7: Eksportere valgt offentlig nøkkel

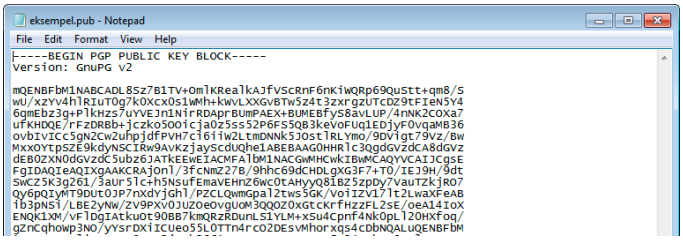
[4] https://www.datatilsynet.no/om-datatilsynet/kryptering-med-openpgp/

3. Naviger frem til lokasjonen der du vil lagre eksporteringen av din offentlige nøkkel.
4. Navngi filen, for eksempel bedriftnavn.pub.asc. Husk å legge til filtypen *.pub.asc* i navnet for å lettere identifisere filen.



Figur 8: Navngi eksport av offentlig nøkkel

5. Du kan åpne denne eksporterte offentlige nøkkelen i Notepad for å forsikre deg om at den er korrekt.
6. En korrekt generert eksport av en offentlig nøkkel vil starte med teksten **-----BEGIN PGP PUBLIC KEY BLOCK-----** som vist på i figur 9.



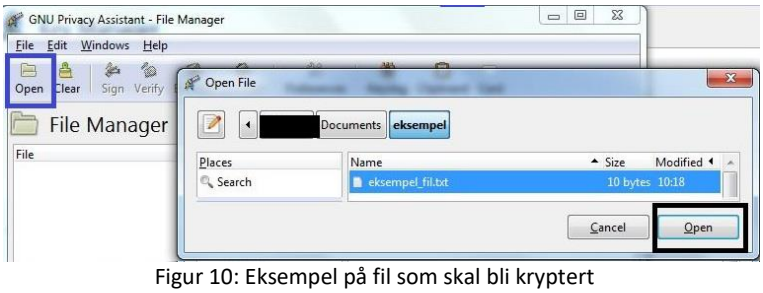
Figur 9: Eksempel på en eksportert offentlig nøkkel

7. Du kan dele denne filen med andre for kryptert og autentisert kommunikasjon.

Mottager bør bekrefte at han har mottatt riktig nøkkel fra deg ved å få deg til å oppgi fingerprint for nøkkelen din.

Kryptering en fil før utsendelse

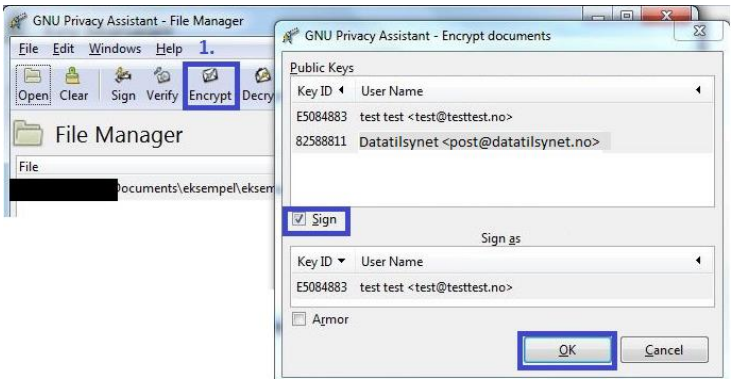
1. Åpne File Manager-visningen fra ved å velge denne fra Windows-valget i menylinjen.
2. Klikk Open-ikonet i File Manager-vinduet.



Figur 10: Eksempel på fil som skal bli kryptert

3. Naviger frem til filen du vil kryptere, merk den, og klikk Open.
4. Klikk Encrypt-ikonet i File Manager-vinduet.
5. Klikk Velg nøkler for kryptering. Alle som skal kunne dekryptere filen må være valgt her. Dette betyr at du i tillegg til mottager må velge din egen nøkkel dersom du ønsker å kunne dekryptere den krypterte versjonen av filen på et senere tidspunkt.

6. Huk av for signering og klikk OK.

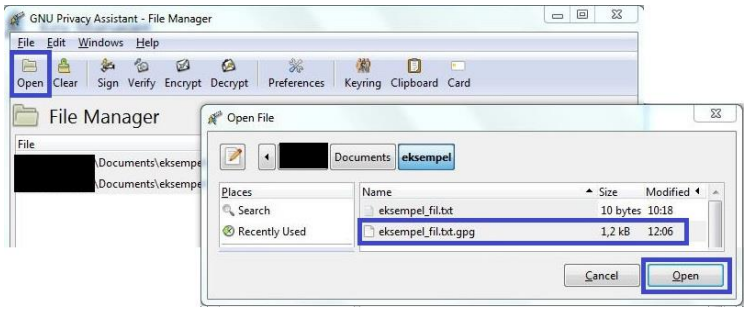


Figur 11: Eksempel på fil som skal bli kryptert

7. Oppgi passordet for den private nøkkelen når du blir spurt om dette.
8. Den krypterte filen vil legge seg i samme mappe som originalfilen, men med *.asc* eller *.gpg* som filendelse.

Dekryptere fil

1. Åpne File Manager-visningen.
2. Klikk Open i File Manger-vinduet.



Figur 16: Dekryptere fil

3. Naviger frem til filen som skal dekrypteres, merk filen og klikk Open.
4. Oppgi eventuelt passord for nøkkelen din når du blir bedt om det.
5. Den dekrypterte filen vil bli lagret i samme katalog som den krypterte filen.